Remarks

1) Rejections under 37 CFR 1.75 & 35 USC 112

The Examiner objected to the specification under 37 CFR 1.75 (d)(1) for failing to provide support for the subject matter recited in claim 35. Claim 35 has been rejected under 35 USC 112 for the same reason. Applicants have cancelled claim 35 from this application and the Examiner's rejections are now believed to be moot.

2) Formality Objection

Applicants have amended the informality pointed out by the Examiner in claim 1, in accordance with the Examiner's suggestion.

3) Rejections under 35 USC 103

The Examiner has rejected claims 1 and 31 to 37 under 35 USC 103 as being unpatentable over Shinn (U.S. 6,655,585) in view of Collberg (U.S. 6,668,325).

Applicants have amended step d) of claim 1 to recite that the step of performing tamper-resistant software (TRS) encoding to the access software application includes storing the biometric data of the user in an encoded format that is irreversible. Support for this feature is found in at least paragraphs [0040] item 1 last 3 lines, item 2 last 4 lines, and item 3 lines 4 to 7, [0041] lines 3 to 4, [00125] lines 2 to 5, [00138], [00139], [00140], and [00134] item 2 lines 2 to 4.

Applicants respectfully submit that neither Shinn nor Collberg discloses integrating into the access software application, by means of partial evaluation, the parameters and the biometric template, and performing tamper-resistant software (TRS) encoding to the access software application including storing the biometric data in an encoded format that is irreversible.

It is well known in the art that the biometric data of a user can never be used again if compromised or stolen (see background of the invention at paragraph [0014]). The invention provides a solution to this problem by storing the biometric data obtained from the user on the access software in an encrypted form (see paragraph [00125]). Paragraph [00134] teaches that if the biometric data has been TRS-encoded with the access software, it is impossible to

reverse-engineer the biometric data back to its original format. Paragraph [00138] teaches that if the PDA, laptop, blackberry or similar device is stolen the biometric data is protected. The attacker may be able to access the TRS-encoded code, but will not be able to obtain any biometric data in real-world format. According to paragraph [0040], secure hardware is not needed as there is no biometric data stored in an unprotected form anywhere in the system.

Shinn discloses a method for authenticating a smart card user at a reader device. The method includes collecting biometric samples from the user and comparing the samples with one or a plurality of stored templates, in order to allow or deny access according to a certain threshold match.

Shinn fails to teach or suggest storing the biometric data of the user in an encoded format that is irreversible. Column 2 lines 62 to 67 of Shinn disclose that the system enhances security by eliminating the necessity of transmitting the user's biometric template to different locations.

In contrast, amended claim 1 recites storing the biometric data in an encoded format that is irreversible. Therefore, if the PDA, laptop, blackberry or similar device is stolen the biometric data is protected. The attacker may be able to access the TRS-encoded code, but will not be able to obtain any biometric data in real-world format (see paragraph [00138]).

Accordingly, Shinn fails to teach integrating into the access software application, by means of partial evaluation, the parameters and the biometric template, and performing tamper-resistant software (TRS) encoding to the access software application including storing the biometric data in an encoded format that is irreversible, as recited in claim 1.

Collberg discloses obfuscation techniques for enhancing software security, including obfuscating a selected subset of code. The code can be obfuscated for enhanced software security based on a desired level of obfuscation (see Abstract). According to Collberg, deobfuscation resembles partial evaluation in that the dynamic part corresponds to the original unobfuscated program and the static part corresponds to the bogus inner program (column 31, lines 46 to 53, and claims 5 and 10).

Collberg fails to teach or suggest integrating the parameters of the access software application and the biometric template into the access software application by means of partial evaluation. Instead, the system of Collberg uses partial evaluation in the deobfuscation process (see column 3 lines 17 to 20, and claims 5, 10, and 15) not in the obfuscation process as taught and claimed herein.

Moreover, Collberg suggests the use of a partial evaluator in order to avoid poor run-time performance because it is known in the art that a partial evaluator evaluates as much of a program as possible using the static data and outputs a specialized residual program to be completed when the dynamic is received (see page 4 of the document entitled "*C++ Templates as Partial Evaluation"* published on November 2, 1998, which can be found at the following link http://arxiv.org/PS_cache/cs/pdf/9810/9810010v2.pdf or by searching for "partial evaluation on http://en.wikipedia.org/wiki/Partial_evaluation).

In contrast, claim 1 recites integrating into the access software application, by means of partial evaluation, the parameters and the biometric template, and performing tamper-resistant software (TRS) encoding to the access software application. Partial evaluation is used in the present invention for inserting the actual parametric and biometric data values into functions and equations in the access software code, before reducing the code and performing the TRS encoding (see paragraph [0040] item 1 lines 8 to 11). Paragraph [00134] teaches that if the biometric data has been TRS-encoded with the access software, it will be impossible to reverse-engineer the biometric data back to its original format.

Accordingly, Collberg fails to teach integrating into the access software application, by means of partial evaluation, the parameters and the biometric template, and performing tamper-resistant software (TRS) encoding to the access software application including storing the biometric data in an encoded format that is irreversible, as recited in claim 1.

Accordingly, the combination of Shinn and Collberg fails to teach or suggest each and every element of claim 1. Withdrawal of the rejection under 35 U.S.C. 103 (a) is respectfully requested.

Claims 31 to 34 and 36 to 37 are believed to be allowable at least in view of their direct or indirect dependency on claim 1.

Accordingly, claims 1, 31 to 34 and 36 to 37 are believed to be in compliance with 35 USC 103 (a) and withdrawal of the rejections is respectfully requested.

The Application is now believed to be in condition for allowance, and early action in that respect is courteously solicited.

A Power of Attorney was filed on August 7, 2008, appointing the attorneys associated with Customer No. 26123.

The Commissioner is hereby authorized to debit $810.00 from Deposit Account No. 501593, in the name of Borden Ladner Gervais LLP, representing the fees for a Request for Continued Examination (RCE).

The Commissioner is hereby authorized to charge any additional fees, and credit any over payments to Deposit Account No. 501593, in the name of Borden Ladner Gervais LLP.

Respectfully submitted,

JOHNSON, Harold, J. et al

By: /Anne Kinsman/

Anne Kinsman
Reg. No. 45,291
Borden Ladner Gervais LLP
World Exchange Plaza
100 Queen Street, Suite 1100
Ottawa, ON K1P 1J9
CANADA
Tel: (613) 237-5160
Fax: (613) 787-3558
E-mail: ipinfo@blgcanada.com

ALK/IT/cf/alc